UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,994	12/27/2000	Douglas B. Quine	F-240	6431

919 7590 04/30/2008

PITNEY BOWES INC.
35 WATERVIEW DRIVE
P.O. BOX 3000
MSC 26-22
SHELTON, CT 06484-8000

EXAMINER	
LEE, TOMMY D	
ART UNIT	PAPER NUMBER
2625	

MAIL DATE	DELIVERY MODE
04/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/748,994
Filing Date: December 27, 2000
Appellant(s): QUINE, DOUGLAS B.

George M. Macdonald
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed February 6, 2008 appealing from the Office action mailed September 6, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

No evidence is relied upon by the examiner in the rejection of the claims under appeal.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1, 5, 7, 12-23 and 25 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,438,433 (Reifman et al., hereinafter Reifman) in view of U.S. Patent 6,170,744 (Lee et al., hereinafter Lee).

For claim 1, Reifman teaches a method of authenticating information communicated between a first communication device and a second communication device via a communications network, comprising the steps of: a. receiving input data and generating facsimile information in a first format by said first communication device from said input data; b. processing said input data to compute an encrypted checksum; c. convolving said facsimile information with said encrypted checksum data to produce convolved data (Col 23 Line 68-Col 24 Line 16); d. decrypting, at said second communication device, said encrypted checksum; e. computing a checksum of said input data received at said second communications device; and f. alerting a recipient at said second communication device in the event of a mismatch between said checksum data computed in step (e) and said decrypted checksum data in step (d) by clearly marking the received input data indicating a tamper condition (Col 48 Lines 48-59).

Claim 1 has been amended to now recite the step of "clearly marking *a print out of* the received input data indicating a tamper condition." It does not appear that

Reifman teaches or suggests overlaying a tamper indication message on the fax print out. However, the clear marking of a tampered document is well known in the art. Lee discloses a method wherein a checksum is computed on a decrypted document, and if there is a mismatch, the document is flagged as possibly fraudulent or corrupt and marked for further intervention (column 12, line 54 – column 13, line 3). The clear marking of the document in such a manner enables a person receiving the document to determine that a document may be corrupted simply by looking at it, thereby avoiding confusion that may arise if there were no marking on the document. Therefore, it would have been obvious for one of ordinary skill in the art, at the time of applicant's invention, to have modified the teaching of Reifman, by providing a step for clearly marking the corrupted document, as taught by Lee.

Regarding claim 5, Reifman teaches the method of claim 4, wherein a database system is communicatively coupled to said second communication device (Col 51 Lines 3-6).

Considering claim 7, Reifman teaches the method of claim 1, further comprising the step of: configuring an e-mail system for receiving and displaying an alert message to said recipient along with said received input data (Col 61. Lines 7-10; EFAX).

For claim 12, Reifman teaches wherein the convolved data is transmitted to the second facsimile communication devices as an e-mail attachment (Col 48 Lines 60-64).

For claim 13, Reifman discloses sending the convolved data to a third facsimile communication device (Col 1 Lines 44-54; Col 3 Lines 41-51).

Considering claim 14, Reifman discloses receiving a user name and password from a user with the second facsimile communication device (Col 10 Lines 33-39).

Considering claim 15, Reifman discloses a method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of: receiving at the second facsimile communications device via a communication network, comprising the steps of: receiving at the second facsimile communications device transmitted data including a digital representation of the entire facsimile document and convolved encrypted authentication data associated with the digital representation of the entire facsimile document in a first format sent by said first communication device (Col 23 Line 68- Col 24 Line 16); processing said transmitted data ,at said second communication device, to extract a digital representation of the entire facsimile document and convolved encrypted authentication data; decrypting, at said second communication device, said encrypted authentication data; computing, at said second communication device, a comparison version of the authentication data using the digital representation of the entire facsimile document and convolved encrypted authentication data; and alerting a recipient at said second communication device in the event of a mismatch between said authentication data and said comparison version of the authentication data by clearly marking the received input data indicating a tamper condition (Col 48 Lines 48-59).

Claim 15 has been amended to now recite the step of "clearly marking *a print out of* the received input data indicating a tamper condition." As mentioned above with

respect to claim 1, it does not appear that Reifman teaches or suggests overlaying a tamper indication message on the fax print out. However, the clear marking of a tampered document is well known in the art. Lee discloses a method wherein a checksum is computed on a decrypted document, and if there is a mismatch, the document is flagged as possibly fraudulent or corrupt and marked for further intervention (column 12, line 54 – column 13, line 3). The clear marking of the document in such a manner enables a person receiving the document to determine that a document may be corrupted simply by looking at it, thereby avoiding confusion that may arise if there were no marking on the document. Therefore, it would have been obvious for one of ordinary skill in the art, at the time of applicant's invention, to have modified the teaching of Reifman, by providing a step for clearly marking the corrupted document, as taught by Lee.

For claim 16, Reifman teaches the method of claim 4, wherein a database system is communicatively coupled to said second communication device (Col 51 Lines 3-6).

Regarding claim 17, Reifman teaches further comprising the step of: configuring an e-mail system for receiving and displaying an alert message to said recipient along with said received input data (Col 61 Lines 7-10; EFAX).

Considering claim 18, Reifman discloses wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes a printing a clear mark across a print out of the received input data indicating a

tamper condition (Col 48 Lines 35-37,52-56 and Col 49 Lines 12-18; user has option to choose "print on the IFAX").

For claim 19, Reifman teaches wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes displaying a clear mark across a computer display of the received input data indicating a tamper condition (Col 47 Lines 64-65 and Col 48 Lines 52-56).

Regarding claim 20, Reifman teaches wherein the convolved data is transmitted to the second facsimile communication devices as an e-mail attachment (Col 48 Lines 60-64).

Considering claim 21, Reifman discloses sending the convolved data to a third facsimile communication device (Col 1 Lines 44-54; Col 3 Lines 41-51).

For claim 22, Reifman discloses receiving a user name and password from a user with the second facsimile communication device (Col 10 Lines 33-39).

For claim 23, Reifman teaches a method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of: receiving at the second facsimile communications device transmitted data including a digital representation of the entire facsimile document and convolved encrypted authentication data associated with the facsimile document and consisting of a single encrypted checksum of the entire facsimile document in a first format sent by said first communication device; processing said transmitted data, at said second communication device, to extract a digital representation of the entire facsimile document and

convolved encrypted authentication data (Col 23 Line 68- Col 24 Line 16); decrypting, at said second communication device, said encrypted authentication data; computing, at said second communication device, a comparison version of the authentication data using the a digital representation of the entire facsimile document and convolved encrypted authentication data; and alerting a recipient at said second communication device in the event of a mismatch between said authentication data and said comparison version of the authentication data (Col 48 Lines 48-59), wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes a clear mark across a print out of the received input data indication a tamper condition (Col 48 Lines 35-37,52-56 and Col 49 Lines 12-18; user has option to choose "print on the IFAX").

Claim 23 has been amended to now recite the step of “printing a mark across a print out of the received input data *clearly* indicating a tamper condition.” As mentioned above with respect to claims 1 and 15, it does not appear that Reifman teaches or suggests overlaying a tamper indication message on the fax print out. However, the clear marking of a tampered document is well known in the art. Lee discloses a method wherein a checksum is computed on a decrypted document, and if there is a mismatch, the document is flagged as possibly fraudulent or corrupt and marked for further intervention (column 12, line 54 – column 13, line 3). The clear marking of the document in such a manner enables a person receiving the document to determine that a document may be corrupted simply by looking at it, thereby avoiding confusion that may arise if there were no marking on the document. Therefore, it would have been

obvious for one of ordinary skill in the art, at the time of applicant's invention, to have modified the teaching of Reifman, by providing a step for clearly marking the corrupted document, as taught by Lee.

Regarding claim 25, Reifman discloses the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes displaying a clear mark across a computer display of the received input data indicating a tamper condition (Col 47 Lines 64-65 and Col 48 Lines 52-56).

(10) Response to Argument

Argument 1:

"Initially, Appellant respectfully submits that the references are not properly combined. Lee '744 requires the use of physical documents that are physically generated at the source and would not be operable in combination with a facsimile system. The two references are not analogous since Reifman '433 deals exclusively with electronic facsimile document transmission and Lee '744 deals exclusively with physical document transport. Accordingly, one of skill in the art would not look to Lee '744 in order to modify Reifman '433." (Appeal Brief: page 9, line 26 – page 10, line 4).

Response:

In response to Applicant's argument that Reifman and Lee are nonanalogous art, it has been held that a prior art reference must either be in the field of Applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the Applicant was concerned, in order to be relied upon as a basis for rejection of the

claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992).

Reifman teaches decryption of an incoming message that had previously been encrypted. A hash code is computed for the incoming data. An incoming hash code corresponding to the incoming message is decrypted, and is compared with the computed hash code. If they are not equal, then an error report is entered into an Error Log. (Reifman: column 48, lines 48-56).

Lee teaches the use of a public key to decrypt a data packet that was previously encrypted. A checksum value had been stored as data in the packet, and this checksum is compared with a computed checksum once the data is decrypted. If they do not match, the document is flagged as possibly fraudulent or corrupt, and marked for further intervention (Lee: column 12, line 54 – column 13, line 3).

While Reifman may deal with electronic document transmission and Lee may deal with physical document transport, it is clear that the references are analogous in that each teach computation of some type of code associated with received data which had previously been encrypted, and comparison of the computed code with code data associated with the received data that has been decrypted to determined whether or not the received data had been tampered with. Therefore, these references are properly combined.

Argument 2:

"Furthermore, any marking system of Lee '744 that were to be combined with Reifman '433 would not be capable of printing the entire document at the destination

and thus the combination would not be operable or at least not suitable for its intended purpose. Moreover, it appears that the system of Lee '744 does not create a digital signature of an entire document. (Appeal Brief: page 10, lines 5-9).

Response:

Applicant's claims merely require that a print out of the received input data indicating a tamper condition be clearly marked. Lee states: "Once the data is decrypted, a checksum is computed and compared against the checksum value stored as data in the packet in step 445. If they do not match, as determined in step 448, the **document** is flagged as possibly fraudulent or corrupt and **marked** for further intervention, as noted in step 449." (Lee: column 12, line 65 – column 13, line 3, emphasis added).

Argument 3:

"The cited references do not appear to describe convolving the data as claimed and marking a print out of received input data." (Appeal Brief: page 11, lines 7-8).

Response:

Reifman states: "The IFAX 10 permits encryption of a facsimile message by selecting an "Encryption" button 190. In addition, the IFAX 10 permits the transmission of a digital signature by selecting a "Digital Signature" button 192, and an authentication option by selecting an "Authentication" button 194. **The digital signature causes the IFAX 10 to transmit a checksum or other data portion in encrypted form along with the encrypted facsimile message.**" (Reifman: column 23, line 68 – column 24,

line 8, emphasis added). This reads on Applicant's step of "convolving said facsimile information with said encrypted checksum data to produce convolved data."

Lee clearly teaches Applicant's step of "clearly marking a print out of the received input data indicating a tamper condition," as mentioned in the above response to Argument 2.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Thomas D Lee/

Primary Examiner, Art Unit 2625

Conferees:

Edward Coles,

/Edward L. Coles/
Supervisory Patent Examiner, Art Unit 2625

Twyler Haskins

/Twyler L. Haskins/
Supervisory Patent Examiner, Art Unit 2625